E-Mails verschlüsseln und digital unterschreiben

Das E-Mail-Client-Programm *Thunderbird* lässt sich mit dem Programm *GnuPG* und dem Add-On[1] *Enigmail* um Funktionen zum Verschlüsseln und digitalen Unterschreiben von E-Mails erweitern.

Schritt 1: Sicherstellen, dass alle Programme installiert sind

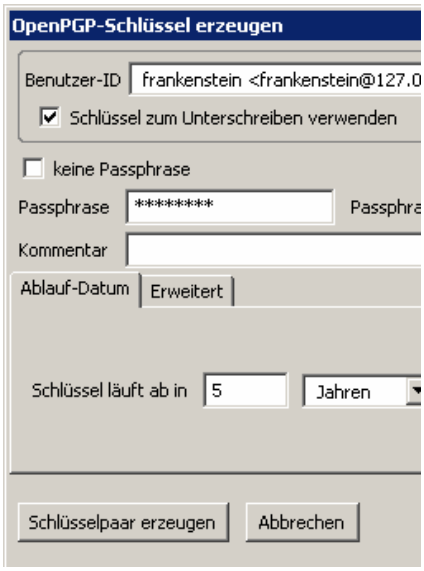
Um E-Mails mit *Thunderbird* verschlüsseln und digital unterschreiben zu können müssen folgende Programme in der angegebenen Reihenfolge auf deinem Computer installiert werden:

A. *Thunderbird* - das Programm kann sich jede(r) lizenzkostenfrei unter http://www.mozillamessaging.com/de/ herunterladen und installieren

B. *Gnu Privacy Guard (GnuPG)*- dieses Programm erledigt die Schlüsselerzeugung, das Ver- und Entschlüsseln, und das Signieren von Nachrichten gemäß dem Open PGP-Standard.
Jede(r) kann sich das Programm für Windows lizenzkostenfrei unter ftp://ftp.gnupg.org/gcrypt/binary/gnupg-w32cli-1.4.10b.exe herunterladen.
(Links zu Versionen für andere Betriebssysteme findest Du unter http://www.gnupg.org/download/index.de.html#auto-ref-2 .)
Ob *GnuPG* auf deinem Computer bereits installiert ist kannst Du herausfinden, indem Du prüfst, ob es im Start-Manü unter Programme bereits einem Ordner „GPG“ gibt!

C. Das *Thunderbird*-Add-On *Enigmail* - ermöglicht es Dir, die Funktionen von *GnuPG* direkt im E-Mail-Client-Programm *Thunderbird* aufzurufen. Das Add-On lässt sich unter https://addons.mozilla.org/de/thunderbird/addon/71/ herunterladen (Wenn Du eine ältere Version von *Thunderbird* hast, klicke auf der Webseite unten auf den Link „Alle Versionen“ und wähle die Version , die zu deiner *Thunderbird*-Version passt!).
Sind *Thunderbird* und *GnuPG* auf deinem Computer installiert, so starte nun *Thunderbird* und rufe im Menü *Extras* → *Add-ons…* auf!
Es öffnet sich ein Dialogfenster „Add-ons“. Klicke auf den Knopf „Installieren“ unten links und wähle die Datei zuletzt heruntergeladene Datei „enigmail … xpi“ aus!
Nach der Installation des *GnuPG*-Add-Ons gibt es in *Thunderbird* einen zusätzlichen Menü-Eintrag „OpenPGP“.

Schritt 2: Schlüsselpaar erzeugen



Sind alle Programme installiert, so solltest Du dir zu allererst ein Schlüsselpaar erzeugen:

1. Wähle im Menü *OpenPGP* → *Schlüssel verwalten* !
2. Wähle im Dialogfenster „OpenPGP-Schlüssel verwalten“ im Menü *Erzeugen* → *Neues Schlüsselpaar* !
3. Wähle nun im Dialogfenster „OpenPGP-Schlüssel erzeugen“ das Postfach aus, für das Du das Schlüsselpaar verwenden möchtest!
4. Darunter solltest Du ein Passwort zweimal eingeben. Das Passwort stellt sicher, dass nur Du deinen privaten Schlüssel benutzen kannst, selbst wenn sich jemand anders (z.B. mit einem Spionage-Programm) Zugang zu der Datei verschafft, in der dein privater Schlüssel gespeichert ist.
5. Erzeuge das Schlüsselpaar durch einen Klick auf den Knopf „Schlüsselpaar erzeugen“!
Durch Speichern des Widerruf-Zertifikats kannst Du den Schlüssel vor Ablauf der Gültigkeit deaktivieren.

[1] Als ein „Add-On“ bezeichnet man eine Erweiterung für ein Programm, die man sich installieren kann, um das Programm mit zusätzlichen Funktionen auszustatten.

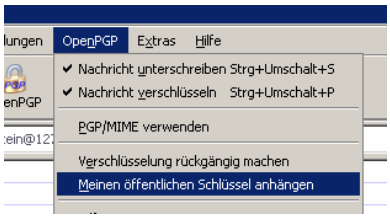
Schritt 3: Öffentliche Schlüssel austauschen

Für den Austausch öffentlicher Schlüssel gibt es zwei Möglichkeiten:

A. Exportiere deinen öffentlichen Schlüssel in eine **Datei**, indem Du
   - im Dialog „OpenPGP-Schlüssel verwalten“ den entsprechenden Schlüssel markierst und
   - im Menü *Datei* → *Exportieren* aufrufst.
   - Natürlich wollen wir den privaten Schlüssel nicht veröffentlichen. Klicke also auf „Nein“, wenn Du danach gefragt wirst. (Die Möglichkeit, den privaten Schlüssel mit zu exportieren ist für den Fall einer Sicherungskopie des Schlüssels gedacht.)
   - Die erzeugte Datei kannst Du nun deinen Kommunikationspartnern übermitteln (z.B. auf einen USB-Stick kopieren, auf deine private Homepage hoch laden oder als Anhang in einer E-Mail versenden (Hier sollte aber aus dem Inhalt der E-Mail hervorgehen, dass sie wirklich von Dir stammt).
   - Bekommst Du den Schlüssel von deinem Kommunikationspartner, so kannst Du ihn im Dialog „OpenPGP-Schlüssel verwalten“ über das Menü *Datei* → *Importieren* in die Liste dir bekannter Schlüssel einfügen - wenn Du dir sicher bist, dass das der richtige Schlüssel ist!

B. Veröffentliche deinen öffentlichen Schlüssel auf einem **Schlüssel-Server**, indem Du
   - im Dialog „OpenPGP-Schlüssel verwalten“ den entsprechenden Schlüssel markierst und
   - im Menü *Schlüssel-Server* → *Schlüssel hochladen* aufrufst.
   - Wähle einen der angegebenen Schlüsselserver aus und klicke auf „OK“!
   - Hat dein Kommunikationspartner seinen öffentlichen Schlüssel ebenfalls auf dem Schlüsselserver veröffentlicht, so kannst Du ihn über das Menü *Schlüssel-Server* → *Schlüssel suchen* durch Eingabe seiner E-Mail-Adresse suchen.
   - Markiere den Eintrag mit der korrekten E-Mail-Adresse und klicke auf „OK“, um den Schlüssel in die Liste dir bekannter Schlüssel einfügen.

Schritt 4: E-Mails verschlüsseln und digital unterschreiben



Haben Absender und Empfänger ihre Schlüssel einmal wie oben beschrieben ausgetauscht, so wird und das eigentliche Verschlüsseln und digitale Unterschreiben der E-Mails von *Enigmail* leicht gemacht:

- Zum Verschlüsseln einer E-Mail klicke nach dem Verfassen der E-Mail im Menü *OpenPGP* auf den Eintrag *Nachricht verschlüsseln*. Der Haken vor diesem Menüeintrag zeigt, dass die Verschlüsselung aktiviert ist. Möchtest Du die E-Mail doch nicht verschlüsseln, so klicke einfach erneut auf den Menüeintrag *OpenPGP* → *Nachricht verschlüsseln* um den Haken zu entfernen.

- Zum digitalen Unterschreiben einer E-Mail klicke nach dem Verfassen der E-Mail im Menü *OpenPGP* auf den Eintrag *Nachricht unterschreiben*. Fortan ist ein Haken vor diesem Menüeintrag gesetzt, das Verschlüsseln ist also aktiviert. Möchtest Du die E-Mail doch nichtunterschreiben? Dann klicke einfach erneut auf den Menüeintrag *OpenPGP* → *Nachricht unterschreiben* um den Haken zu entfernen.
  Über den Menüeintrag *OpenPGP* → Meinen *öffentlichen Schlüssel anhängen*“ kannst Du übrigens bequem deinen öffentlichen Schlüssel der E-Mail als Dateianhang hinzufügen.

Hinweis: Das Absenden einer **verschlüsselten** Nachricht gelingt natürlich nur, wenn der öffentliche Schlüssel zur **E-Mail-Adresse des Empfängers** bekannt ist.
Unterschreiben kann ich dagegen jede E-Mail, es liegt dann am Empfänger, ob er die Unterschrift mit meinem öffentlichen Schlüssel überprüfen möchte oder nicht.

Aufgabe: Starte wie zu Beginn dieser Unterrichtsreihe das Netzwerkanalyseprogramm *Socket Sniff*! Erzeuge dir ein Schlüsselpaar, tausche deinen öffentlichen Schlüssel mit anderen Mitschülern und versendet Euch verschlüsselte und digital unterschriebene E-Mails! Betrachtet den E-Mail-Verkehr in *Socket Sniff*! Wie schlau werden nun neugierige Angreifer, die sich Zugang zu Routern oder dem E-Mail-Server verschaffen aus Euren E-Mails?!